UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/593,280	06/13/2000	Cheuk W. Ko	NA00-02401	7783

28875 7590 02/10/2004

SILICON VALLEY INTELLECTUAL PROPERTY GROUP
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
HENEGHAN, MATTHEW E	
ART UNIT	**PAPER NUMBER**
2134	7

DATE MAILED: 02/10/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application	Applicant(s)	
	09/593,280	KO, CHEUK W.	
	Examiner	Art Unit	
	Matthew Heneghan	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 December 2003*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Applicant's response to the first office action, including amendments and corrected drawings, was received by the Office on 11 December 2003. Claims 1, 4-8, 10, 11, 13-17, 19, 20, 22, 24, and 26 have been amended.

2. Claims 1-27 have been examined.

Drawings

3. The corrected drawings were received on 11 December 2003. These drawings are acceptable.

Claim Objections

4. In view of applicant's amendments filed 11 December 2003, all existing claim objections are withdrawn.

Claim Rejections - 35 USC § 112

5. In view of applicant's amendments filed 11 December 2003, all existing rejections under 35 U.S.C. 112 are withdrawn.

Regarding claims 4, 6, 13, 15, 22, and 24, the list of items in each claim is now being treated as an open-ended set of limitations, necessitating new grounds of rejection under 35 U.S.C. 103, below.

Claim Rejections - 35 USC § 102

6. Due to modifications to the claims in applicant's amendments filed 11 December 2003, all previous rejections under 35 U.S.C. 102 are replaced by rejections under 35 U.S.C. 103, below.

Claim Rejections - 35 USC § 103

7. Claims 1-3, 7-12, 16-21, and 25-27 are rejected 35 U.S.C. 103(a) as being unpatentable over U.S Patent No. 5,557,742 to Smaha et al. in view of U.S. Patent No. 5,513,317 to Borchardt et al.

As per claims 1, 8, 10, 17, 19, and 26, the intrusion detection system disclosed by Smaha receives an audit trail, stores specified data in an event data structure(60), compares data against the contents of the information modules(62,64,66) using complete query(84) and compares one or more data to criteria for detecting an intrusion (see column 7, lines 8-49). More specifically, a misuse engine is employed that uses queries stored in a signature data structure(108) to determine intrusions (see column 9, line 31 to column 10, line 45).

More specifically, an audit specification ("selected misuses") is received, specifying one or more misuses, wherein a misuse is a target attribute (see column 9, line 31-48 and Figures 3, 4, and 5a). The selected misuses trigger "events" when detected (see column 10, lines 1-10). A report is generated in the event of an event matching the defined attributes (see column 10, lines 41-45). The log is examined for intrusion detection purposes (see column 10, lines 24-32 and title of patent).

Smaha does not disclose the reducing of the size of the audit log prior to examination.

Borchardt discloses a trace filter in which data is filtered according to one or more attributes before being analyzed by the programmer (see column 4, lines 1-19), and suggests that the volume of information provided by a trace facility can grow to such large proportions as to obscure the few relevant pieces of information that the trace facility has captured (see column 1, lines 56-59).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the system disclosed by Smaha by filtering according to one or more attributes before being analysis, as disclosed by Borchardt, as the volume of information provided by a trace facility can grow to such large proportions as to obscure the few relevant pieces of information that the trace facility has captured.

As per claims 2, 9, 11, 18, 20, and 27, Smaha discloses that programs can be used to dynamically select misuses based on a set of criteria (see column 9, lines 15-20).

As per claims 3, 12, and 21, Smaha discloses that the signature information structure is initialized in a UNIX™ system by retrieving it from disk storage (see column 12, lines 5-40). Official notice is given that it is well-known in the art that all transactions with disk storage in the UNIX™ operating system are necessarily performed using one of a number of system calls, such as read(), open(), and close().

Smaha does not specifically disclose the use of jump tables for choosing the appropriate system calls for performing file I/O.

Official notice is given that it is well-known in the art that the method of using a jump table is an efficient way, both in terms of execution speed and memory usage, to specify a jump or call to one of a list of processes in a situation where the decision can be made based upon the value of an single integer variable, such as an index, and that jump tables can be dynamically modified, based upon changing conditions.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to implement the system disclosed by Smaha by using a system call jump table, in order to efficiently choose the correct the correct system call by which to retrieve the signature information structure from disk storage.

Regarding claims 7, 16, and 25, the filtering of data from an audit log inherently reduces the amount of data stored in it, as the removal of data from files always makes them smaller.

8. Claims 4, 6, 13, 15, 22, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S Patent No. 5,557,742 to Smaha et al. in view of U.S. Patent No. 5,513,317 to Borchardt et al. as applied to claim 1 above, and further in view of U.S. Patent No. 6,584,508 to Epstein et al. further in view of Kernighan et al., "The UNIX Programming Environment," 1984.

Smaha and Borchardt do not disclose the analysis of other data relevant to logged system calls in the misuse engine.

The data guard system disclosed by Epstein includes the ability to screen a variety of system call attributes by using wrappers around system calls, so that any parameter to the system call may be intercepted (see column 5, lines 32-55). Epstein further discloses that intercepted calls might include an exec call, for which the name of a process is passed as a parameter, or an attempt to read a file, for which a parameter must be an identifier for the calling application program (see column 6, lines 58-67). Epstein further suggests that the software wrappers provide for relatively small specifications of the allowed behavior of associated multi-part proxy components, and security of firewall components is thereby improved (see column 3, lines 29-32).

Regarding claims 4, 13, and 22, Epstein does not completely detail the attributes that are included in system calls, but states that all system calls may be intercepted, along with all associated parameters ("arguments").

Regarding claims 6, 15, and 24, Epstein states the auditing criteria can include a specific user or directory, which is a type of file (see column 5, lines 56-60), or any other attribute extractable from system calls, but does not specifically

specify the screening by the application from which the system call is being made.

Kernighan discloses that systems calls may contain information about the process making the system call, from argv[] (see pp. 174 and 217) or the file descriptor or the data buffer for reading or writing (see p. 202). Since all peripheral devices use file descriptors in system calls (see p. 201) and UNIX is a network operating system used on computers wherein peripherals (such as Ethernet cards) are used for network communications, it is inherent that parameters may also be related to network communications.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the intrusion detection system disclosed by Smaha and Borchardt by implementing software wrappers for the system calls, making the parameters of system calls available for auditing, as disclosed by Epstein, screening all UNIX system call parameters disclosed by Kernighan, thereby improving the security of firewall components.

9. Claims 5, 14, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S Patent No. 5,557,742 to Smaha et al. in view of U.S. Patent No. 5,513,317 to Borchardt et al. as applied to claim 1 above, and further in view of U.S. Patent No. 5,623,601 to Vu.

Smaha and Borchardt do not disclose the incorporation of the misuse engine into the operating system's kernel.

Vu discloses a system for secure gateway communications that includes the incorporation of the engine directly in the operating system kernel (see column 4, lines 51-64), and further notes that data communications are delivered to the application level through the kernel (see column 6, lines 2-13).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to incorporate the misuse engine disclosed by Smaha and Borchardt into the operating system kernel, as disclosed by Vu, as all data communications are delivered to the application level through the kernel.

Response to Arguments

10. Applicant appears to be traversing the official notice taken in paragraph 8 of paper #6. This traverse is inadequate as it does not point out the supposed errors in that action as required by MPEP 2144.03, in part, as follows:

> To adequately traverse such a finding, an applicant must specifically point out the supposed errors in the examiner's action, which would include stating why the noticed fact is not considered to be common knowledge or well-known in the art.

Applicant's response has failed to specifically point out any supposed errors in the official notice that has been taken, and no reasoning has been presented that would in any way suggest that an error has been made by the Office. The Office is therefore in no way obligated to present evidence that the cited features are well known to those of ordinary skill in the art. As a one-time

courtesy, however, relevant documentation with respect to those features is referenced below.

In any future responses to office actions with respect to this invention, applicant shall be required to seasonably traverse, when appropriate, all inappropriate use of official notice with accompanying reasons that the official notice is thought to be in error.

Regarding the official notice given that it is well-known in the art that all transactions with disk storage in the UNIX™ operating system are necessarily performed using one of a number of system calls, such as read(), open(), and close(), the office cites, Kernighan et al., "The UNIX Programming Environment," 1984, pp. 201-206. On p. 201, Kernighan states that:

> All input and output is done by reading or writing files, because all peripheral devices, even your terminal, are files in the file system. This means that a single interface handles all communication between a program and peripheral devices.

The single interface in UNIX™ is the set of system calls, several of which are described in the reference.

Regarding the official notice is given that it is well-known in the art that the method of using a jump table is an efficient way, both in terms of execution speed and memory usage, to specify a jump or call to one of a list of processes in a situation where the decision can be made based upon the value of an single integer variable, such as an index, and that jump tables can be dynamically modified, based upon changing conditions, the office cites U.S. Patent No. 4,713,754. Jump tables (also known as "vector tables" or "pointer tables") are

explicitly supported by most modern microprocessors by way of the "indexed indirect" addressing mode in jump, branch, and call commands. Agarwal discloses that the speed of execution can be enhanced by using a Software Interrupt Vector Table (see column 8, lines 6-12).

Regarding the official notice is given that the method of filtering unwanted information from a file in order to reduce its size is well-known in the art, the change in the reasons for rejections, above, renders this notice moot.

11. Applicant's arguments filed 11 December 2003 have been fully considered but they are not persuasive.

Regarding applicant's arguments, all limitations of applicant's original claims rejected under 35 USC 102(b) are found to have been anticipated by Smaha. As discussed above, Smaha does produce an audit log, which is examined for intrusion detection purposes; Smaha further elaborates on the outputting of detected misuses in column 10, line 55 to column 11, column 23, wherein it may be recorded if configured to do so.

Regarding rejections to claims under 35 USC 103(a) over Smaha in view of Epstein, the rejection has been changed in view of applicant's amendments in response to previous rejections under 35 USC 112, second paragraph, as all items in the claim are now being viewed as limitations. In view of the additional art, Kernighan, the claims remain rejected.

Conclusion

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (703) 305-7727. The examiner can normally be reached on Monday-Thursday from 8:00 AM - 4:00 PM Eastern Time. The examiner can also be reached on alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
Washington, DC 20231
Or faxed to:
(703) 872-9306
Hand-delivered responses should be brought to Crystal Park 2, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

MEH

February 5, 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100